☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Dyna Abu Hamdha's person (DOB: 05/1991), residences and vehicles; See Attachments

Case No. 23 MJ 130
Matter No.: 2023R00184

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A; over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 8/14/2023 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. William E. Duffin.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/1/2023 at 11:31 AM

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Matter No. 2023R00184

The person to be searched pursuant to this warrant is Dyna Abu HAMDHA (F/W; DOB: 05/18/1991).

The places to be searched pursuant to this warrant are residences and conveyances utilized by HAMDHA; specifically:

a) 5890 Tower Road, Apartment 4, Greendale, WI (Target Residence-1);
   - Target Residence-1 is an apartment unit (No. 4) located on second floor within the southwest quadrant of the apartment complex located at 5890 North Tower Road. The main entrance to the encompassing building is located on the west side of the apartment complex, facing Tower Road. The entry door of Target Residence-1 is located directly across a small hallway from Target Residence-2.

b) 5890 Tower Road, Apartment 3, Greendale, WI (Target Residence-2);
   - Target Residence-2 is an apartment unit (No. 3) located on second floor within the northwest quadrant of the apartment complex located at 5890 North Tower Road. The main entrance to the encompassing building is located on the west side of the apartment complex, facing Tower Road. The entry door of Target Residence-2 is located directly across a small hallway from Target Residence-1.

c) 2023 Toyota Camry WI license plate "AFH5270" (Target Vehicle-1)
   - The Toyota Camry is dark black in color and possesses darkened windows. The vehicle also possesses dark gray/black rims. The vehicle's license plate bears WI tag "AFH5270."

d) 2011 Dodge Grand Caravan WI license plate "ACS6335" (Target Vehicle-2)
   - The Dodge Caravan is white in color, possessing a small amount of rust along the wheel wells and fuel tank inlet. The vehicle's license plate bears WI tag "ASC6335."

Collectively, Target Vehicle-1 and Target Vehicle-2 are the Target Vehicles.

Collectively, Target Residence-1 and Target Residence-2 are the Target Residences.

ATTACHMENT B

Matter No. 2023R00184

Evidence to be seized

All records, information and items, from HAMDHA, the Target Vehicles, or the Target Residences, that relate to violations of 18 U.S.C. §§ 371, 1512, and 1791 and involve Dyna Abu HAMDHA since January 1, 2023, including:

a. Records and information relating to contraband being provided to federal inmates;

b. Records and information relating to controlled substances;

c. Records and information relating to communications between Michael Wright, Ramone Locke, Amanda Deberry, and Dyna Abu Hamdha;

d. Records and information relating to communications with Michael Wright and/or Ramone Locke regarding their pending investigations;

e. Records and information relating to Michael Wright's pending case, Ramone Locke's pending case, or the obstruction of justice;

f. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Amanda Deberry, Michael Wright, Ramone Locke, and Dyna Abu Hamdha;

g. Records and information relating to the identity or location of the suspects, associates, and co-conspirators.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

For any computer or storage medium (including cellular phones) whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

During the execution of the searches described in Attachment A, law enforcement personnel are authorized to obtain from Dyna Abu HAMDHA the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock devices associated with 414-388-9559 and 414-242-1974, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, for the purpose of attempting to unlock 414-388-9559 and 414-242-1974's security features in order to search the contents as authorized by this warrant.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by

any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF or FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Dyna Abu Hamdha's person (DOB: 05/1991), residences and vehicles; See Attachments

Case No. 23 MJ 130

Matter No.: 2023R00184

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A; over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C §§ 371; 1512 and 1791	Conspiracy to commit offense or to defraud United States; tampering with a witness, victim, or an informant; and providing or possessing contraband in prison

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

dalton evertz
Applicant's signature

SA Dalton R. Evertz, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 8/1/2023

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

Matter No. 2023R00184

I, Dalton Evertz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant to seek evidence of conspiracy to commit offense or defraud the United States, in violation of Title 18, United States Code, Section 371; tampering with a witness, victim, or an informant, in violation of Title 18, United States Code, Section 1512; providing or possessing contraband in prison, in violation of Title 18, United States Code, Section 1791 (the "Subject Offenses"). The person to be searched pursuant to this warrant is Dyna Abu HAMDHA (F/W; DOB: 05/18/1991). The places to be searched pursuant to this warrant are residences and conveyances utilized by HAMDHA. The specific residences to be searched are 5890 Tower Road, Apartment No. 4 ("Target Residence-1") and 5890 Tower Road, Apartment No. 3, Greendale, WI, ("Target Residence-2"), collectively referred to hereinafter as the "Target Residences." The specific conveyances to be searched are a black 2023 Toyota Camry bearing WI tag "AFH5270" ("Target Vehicle-1") and a white 2011 Dodge Caravan bearing WI tag "ASC6335" ("Target Vehicle-2"), collectively referred to hereinafter as the "Target Vehicles."

2. I am a Special Agent of the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") currently assigned to the Milwaukee Field Office. As such, I am an investigative or law enforcement agent of the United States authorized under Title 18, United States Code, Section 3051, that is, an officer of the United States who is empowered by law to conduct investigations,

to make arrests, and to collect evidence for various violations of federal law. I have been employed as a Special Agent of the ATF since October 2018.

3. During my tenure with the ATF, I have participated in all aspects of investigations, including executing search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information. Through my experience and training, I have become familiar with activities of individuals engaged in illegal activities, to include their techniques, methods, language, and terms. During my career, my investigations have included the use of various surveillance techniques and the execution of numerous search and seizure warrants, including for computers and cellular telephones.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officials, witnesses, and agencies. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this Affidavit, I submit that there is probable cause to believe that HAMDHA and others have committed violations of the Subject Offenses and that evidence of such crimes is likely to be found in the Target Residences as well as the Target Vehicles, described in Attachment A. As a result, there is probable cause to search the Target Residences, Target Vehicles, and HAMDHA's person, further described in Attachment A, for documents and records, including cellular and electronic devices, described in Attachment B, for evidence of the SUBJECT OFFENSES.

PROBABLE CAUSE

6. The FBI and the ATF are investigating allegations of misconduct, corruption, and obstruction by former Correctional Staff employed by the Waukesha County Sheriff's Office ("WCSO"), who used their positions to provide contraband to federal inmates at the Waukesha County Jail, a correctional facility located in the Eastern District of Wisconsin that maintains an agreement with United States Marshal Service to detain federal prisoners.

The Preceding ATF Investigation: United States v. Locke, et al., 22-cr—133

7. In August of 2021, ATF SAs and Task Force Officers (TFOs) (hereinafter "Case Agents" and/or "Investigators") began investigating an armed drug trafficking organization ("ADTO") operating in the Eastern District of Wisconsin (WI). Over the next eight months, case agents utilized an undercover ATF agent ("UCA") to conduct multiple controlled purchases of cocaine/crack cocaine and dry-meetings with ADTO members. During some of these meetings the members of the ADTO were armed with firearms. Investigators have identified the following individuals as ADTO members: Ramone LOCKE; Joey VAZQUEZ; Alex WEDDLE; Carlos PEREZ-RAMIREZ; Lemar HOWZE; Xzayvier WEDDLE; Gerald JONES; Janicia MACK-HOWARD; and Marisela OBREGON.

8. Between September 1, 2021, and April 28, 2022, the UCA conducted twelve undercover controlled buys from varies member of the ADTO. UCA obtained a total of 140.81 grams (more than five ounces) of crack cocaine and 1316.12 grams (1.316 kilograms) of powder cocaine from the ADTO in this way. Through the undercover controlled buys and investigation into the ADTO, case agents determined that the ADTO used telephone numbers 414-722-0553, 414-517-5178, and 414-627-7500 to conduct their illegal activities. Case agents also identified

telephone number 414-748-7363 as WEDDLE's personal number. All the undercover buys were recorded, and the controlled substances field-tested positive for cocaine. Also, during the undercover controlled buys, the UCA often observed members of the ADTO with additional amounts of suspected controlled substances package to be sold to drug customers.

9. On February 22, 2022, UCA had an undercover meeting with Alex WEDDLE to discuss future drug sales. Alex WEDDLE disclosed, using vernacular/syntax common to drug traffickers, that he communicated with his cocaine source via FaceTime, which is an encrypted video-calling application exclusive to Apple devices (iPhones). Case agents know through training and experience that iPhone users have the option to link an Apple ID/iCloud account to their Apple Devices (i.e., iPhone). iCloud is the service from Apple that stores an account user's photos, files, notes, passwords, messages, and other data in Apple's cloud, and keeps the data/records up to date in all of the user's devices.

10. Beginning in February of 2022, Investigators identified that the ADTO's cocaine source was Ramone LOCKE Sr. based on statements provided by Alex WEDDLE, analysis of FaceTime logs reflecting contact between LOCKE and WEDDLE, jail calls, and database searches. Ramone LOCKE Sr., at that time, employed an Apple iPhone utilizing telephone number 414-578-7810. Further investigative techniques revealed the iCloud account tied to this iPhone was "ramone.locke@icloud.com".

11. On April 22, 2022, Alex WEDDLE, using number 414-748-7363, called UCA via FaceTime. During this FaceTime call, Alex WEDDLE showed UCA a suspected kilogram of cocaine in Alex WEDDLE's possession. This suspected kilogram of cocaine related to the prior

meeting between Alex WEDDLE and UCA had regarding pooling their money together to purchase a kilogram of cocaine from Alex WEDDLE's source.

12. Through FaceTime Call Invitation Log (CIL) records, call detail records (CDRs), historical cellular location data ("pings"), and remote surveillance, Investigators determined LOCKE Sr. had delivered the suspected kilogram to Alex WEDDLE immediately prior to Alex WEDDLE's FaceTime call with the UCA on April 22, 2022.

13. On June 7, 2022, law enforcement located LOCKE Sr. in the Northern District of Illinois, where they observed him, *inter alia*, placing a black bag into his Audi A5. The Audi had a suspected illegal window tint and only bore a rear Wisconsin license plate. Racine County Sheriff Deputies, acting at ATF's direction, stopped the Audi traveling northbound I-94 in Racine County, WI. A search of the vehicle was subsequently conducted, resulting in the Deputies recovering two (2) Apple iPhones and approximately two kilograms of cocaine, which was located inside a sophisticated hidden compartment ("trap"). It is important to note that during the traffic stop, before being detained by Deputies, LOCKE Sr. utilized one of the Apple iPhones recovered from the vehicle to contact HAMDHA via FaceTime. Charges against members of the ADTO are currently pending in *United States v. Locke, et al.*, 22-cr-133 (E.D. Wis.). LOCKE Sr. is currently detained on those charges, after an unsuccessful appeal to United States District Judge Lynn Adelman, who noted that several of LOCKE Sr.'s co-conspirators "suggested that [LOCKE Sr.] would pose a danger to alleged cooperators and their families if released." *Id.* at Dkt. No. 7.

14. Over the course of this investigation, Investigators discerned that LOCKE Sr., Alex WEDDLE, and other members of the ADTO utilized multiple residences, vehicles, and

telephones to carry out their illicit drug trafficking. For example, LOCKE Sr. utilized multiple apartments, not traceable to LOCKE Sr.'s name, in downtown Milwaukee, WI, while LOCKE Sr. also maintained a residence in Greendale, WI. SA Evertz knows through training and experience that narcotics traffickers often possess and/or rent homes, apartments, vehicles, etc., that are listed to family members, associates, and/or fictitious individuals to avoid detection by law enforcement.

Initiation of FBI Investigation; The April 2023 WCSO Tip & Search

15. On April 13, 2023, a clerk at the Waukesha County Jail received a call from a female ("INDIVIDUAL-1") who advised that inmate MICHAEL WRIGHT—a federal inmate who has been in custody at the Waukesha County Jail since October 20, 2021, and is currently awaiting disposition in a multi-defendant case (*See* 21-CR-204) —was in possession of an Apple iPhone. INDIVIDUAL-1 further stated that the iPhone was given to Inmate WRIGHT by staff at the jail. It was determined that Inmate WRIGHT was housed in cell 709, located in Pod 7 at the Waukesha County Jail, and that a search would be conducted of Inmate WRIGHT's cell.

16. During the search of Inmate WRIGHT's cell, which was conducted on April 13, 2023, a Waukesha County Corrections Officer located a pair of white headphones and a white charging cord for an Apple iPhone, hidden inside a fruit snack bag. Jail staff did not locate an Apple iPhone or any other cellular device in Inmate WRIGHT's cell. Inmate WRIGHT was questioned by jail staff about the phone charging cord and headphones, and Inmate WRIGHT eventually admitted that a former Correctional Officer, identified as AMANDA DEBERRY, provided these items to him. Inmate WRIGHT stated that DEBERRY was supposed to bring him

a phone but that she did not do so. Inmate WRIGHT further stated that DEBERRY may have gotten scared and did not follow through with bringing a phone into the jail.

17. In addition to Inmate WRIGHT admitting that DEBERRY provided the phone charging cord and headphones to him, Inmate WRIGHT showed Corrections Staff an email he received via the Waukesha County Jail's messaging service. The email, dated April 8, 2023, identified the sender as "Amanda Deberry" and stated, "Hello Mr Wright long time no see lol would send y a pic but u might show my shit or get in trouble." The message concluded with three emojis commonly referred to as "The Beaming Face with Smiling Eyes."

18. According to information provided by the WCSO, DEBERRY was hired as a Corrections Officer on September 10, 2022. DEBERRY provided telephone number 414-982-9371 as her telephone number. DEBERRY resigned from the WCSO on or about March 23, 2023.

19. According to information received by Sprint pursuant to a subpoena, 414-982-9371 has been subscribed to by DEBERRY since October 5, 2007, with a subscriber address of 3252 North 42nd Street, Milwaukee, WI 53216. An open-source search of the IMEI number associated with 414-982-9371 revealed the device to be an Apple iPhone.

20. After the interview of Inmate WRIGHT, it was determined that a full search of Pod 7, where Inmate WRIGHT's cell was located, would be conducted. Corrections staff eventually located an Apple iPhone in cell 717, occupied by inmate LOCKE, Sr., who has been in custody at the Waukesha County Jail since August 26, 2022, and is currently awaiting trial in his separate multi-defendant federal case. *See* 22-cr-133.

21. Law enforcement obtained a search warrant authorizing the forensic download of the Apple iPhone located in Inmate LOCKE's cell, and the same was conducted by the WCSO.

Based on a review of the forensic download, it appeared the phone was activated on March 22, 2023, at approximately 10:37am and was assigned telephone number 414-885-9950. Of note, the forensic download included numerous communications with telephone number 414-388-9559, to include communications on the day the phone was activated, and over 300 text messages with telephone number 414-242-1974. As described more fully below, both numbers are associated with HAMDHA.

22. According to information received by T-Mobile pursuant to a State of Wisconsin Warrant for Records, 414-388-9559 has been subscribed to by HAMDHA since October 7, 2022, with a subscriber address of 5890 Tower Road, Apartment 4, Greendale, WI 53129 (Target Residence-1). HAMDHA is believed to be a long-time girlfriend of Inmate LOCKE's. An open-source search of the IMEI number associated with 414-388-9559 revealed the device to be an Apple iPhone.

23. According to information received by AT&T pursuant to a State of Wisconsin Warrant for Records, 414-242-1974 has been subscribed to by "Dish Wireless LLC" since January 13, 2023, with a subscriber address of 9601 South Meridian Boulevard, Englewood, CO 80112. An open-source search of the IMEI number associated with 414-242-1974 revealed the device to be an Apple iPhone. As further described below, there is probable cause to believe 414-242-1974 was used by HAMDHA. Additionally, SA Evertz knows through training and experience that individuals engaged in illegal and/or fraudulent activity often falsify their telephone number's subscriber information to avoid detection by law enforcement.

The April 2023 Delivery

24. The WCSO subsequently learned that a vehicle associated with HAMDHA, a black 2023 Toyota Camry (Target Vehicle-1), was located in the area of the Waukesha County Jail on March 22, 2023—the date the device from LOCKE's cell was activated—at approximately 5:40pm. Based on surveillance footage captured by security cameras located on the Waukesha County Campus, where the Waukesha County Jail is located, Target Vehicle-1 was observed parking in the Waukesha County Jail parking lot near the main entrance at approximately 5:45pm. At approximately 6:00pm, while Target Vehicle-1 was parked in the Waukesha County Jail parking lot, DEBERRY was observed exiting the secure confines of the jail and meeting with the operator of Target Vehicle-1, believed to be HAMDHA. DEBERRY obtained a fast-food bag from Chick-Fil-A and a beverage cup from the operator of Target Vehicle-1 and then re-entered the Waukesha County Jail with these items in her possession. DEBERRY was observed returning to her post in Pod 7 with the Chick-Fil-A bag. At approximately 6:12pm, DEBERRY and another Corrections Officer were observed conducting a search of Inmate LOCKE's cell. Of note, while DEBERRY conducted the search of Inmate LOCKE's cell, the other Corrections Officer had his back to DEBERRY in order to monitor the inmates in Pod 7. The search of Inmate LOCKE's cell was concluded at approximately 6:15pm.

25. Based on my training and experience, I know that people commonly communicate and coordinate their schedules using cellular devices. At this time, the investigation has not revealed how DEBERRY and HAMDHA know each other. Despite that, DEBERRY met with the operator of Target Vehicle-1, believed to be HAMDHA, shortly after Target Vehicle-1 arrived at the Waukesha County Jail and was observed bringing a bag containing what is believed to be a

cellphone into the jail for LOCKE. Because people commonly communicate and coordinate their schedules using cellular devices, and because DEBERRY met with the operator of Target Vehicle-1 shortly after it arrived at the Waukesha County Jail, there is probable cause to believe DEBERRY and HAMDHA used their cellular devices (414-982-9371, 414-388-9559, 414-242-1974) to communicate with each other[1] and facilitate the delivery of the device ultimately recovered in LOCKE's cell.

26. A review of the call detail records for 414-388-9559, according to information received by T-Mobile pursuant to a State of Wisconsin Warrant for Records, revealed HAMDHA, using 414-388-9559, communicated with Inmate LOCKE on the cellular telephone that was located in Inmate LOCKE's cell on April 14, 2023. Between March 27, 2023 and April 13, 2023, 414-388-9559 exchanged at least 15 telephone calls or text messages with the cellular telephone that was ultimately located in Inmate LOCKE's cell.

27. A review of the call detail records for 414-242-1974, according to information received by AT&T pursuant to a State of Wisconsin Warrant for Records, revealed HAMDHA, using 414-242-1974, also communicated with Inmate LOCKE on the cellular telephone that was ultimately located in Inmate LOCKE's cell. Between March 25, 2023, and April 13, 2023, 414-

[1] A review of the call detail records for 414-982-9371 for the relevant time period revealed two incoming text messages and one outgoing text message with 414-388-9559, as well as three outgoing telephone calls to Target 414-242-1974; however, these text messages and telephone calls were exchanged on March 23, 2023 – the day after HAMDHA is believed to have provided DEBERRY with the cellular telephone in question. However, a telecommunications provider, such as T-Mobile, cannot provide information about Apple iMessage traffic because iMessages are sent through the internet rather than through a telecommunications provider. As such, there is reason to believe HAMDHA and DEBERRY exchanged additional communications, using their devices, which are not reflected in the call detail records for 414-982-9371, 414-388-9559, and 414-242-1974.

242-1974 exchanged at least 59 telephone calls with the cellular telephone that was located in Inmate LOCKE's cell on April 14, 2023.

28. As previously stated in this Affidavit, a review of the forensic download of the Apple iPhone located in Inmate LOCKE's cell revealed 414-242-1974, believed to be used by HAMDHA, exchanged over 300 text messages with Inmate LOCKE. The text messages exchanged between Inmate LOCKE and HAMDHA using 414-242-1974 revealed that HAMDHA was not only the user of the device, but that she was potentially aware of the relationship between Inmate LOCKE and DEBERRY. For example:

- On April 13, 2023, Inmate LOCKE sent 414-242-1974 an iMessage which stated, "I called both yo phones." Later on April 13, 2023, Inmate LOCKE sent 414-242-1974 an iMessage which stated, "Ok Dyna gn."
- On April 27, 2023, 414-242-1974 sent an iMessage to Inmate LOCKE which stated, "How come you didn't call me." In response, Inmate LOCKE stated, "Dey locked us in early baby." Based on my knowledge of this investigation, I believe "Dey" to be either an abbreviated reference to DEBERRY or a "slang" spelling of "they," meaning the correctional staff.

Reason to Believe 414-388-9559 and 414-242-1974 are located within the Target Residences and/or HAMDHA's Person

29. In my training and experience, people frequently keep their cellular telephones on or very near their person at nearly all times of the day. In my training and experience, when a person's cellular telephone is not on or near their person, it is most often in their vehicles or residences. It is common practice for most people to rely heavily on the use of their cellular telephone for many aspects of their daily lives. Law enforcement also obtained authorization from

The Honorable Nancy Joseph to obtain location data associated with HAMDHA's devices, 414-388-9559 and 414-242-1974. *See* 23-MJ-973. This location data indicates that these devices are frequently located at the Target Residences.

30. There is also reason to believe that HAMDHA frequently uses 414-388-9559 and 414-242-1974, described in Attachment B. For example, on May 23, 2023, according to information received by T-Mobile pursuant to a State of Wisconsin Warrant for Records, 414-388-9559 had approximately 38 incoming/outgoing calls and text messages, consistently throughout the day, between 7:42am CST and 10:02pm CST.

31. With respect to 414-242-1974, based on a review of the forensic download of the Apple iPhone located in Inmate LOCKE's cell, there is reason to believe HAMDHA keeps 414-242-1974 with or very near to 414-388-9559. For example, on April 13, 2023, Inmate LOCKE and 414-242-1974 had the following iMessage exchange, in part:

> Inmate LOCKE: "Y da fuck u not picking up"
>
> 414-242-1974: "Sorry my phone was in my purse sorry"
>
> Inmate LOCKE: "I called both yo phones"
>
> 414-242-1974: "Why are you acting like this I have nothing to lie about"
>
> Inmate LOCKE: "I'm goin 2 sleep"
>
> 414-242-1974: "I promise on everything I been seating in the same spot… My phone was in my purse both of them I just went to look at them and seen you was calling"

32. Law enforcement has currently paused its review of the cellphone recovered from Inmate LOCKE's cell, after reviewing messages that are believed to be exchanged by Inmate

LOCKE and a third-party regarding Inmate LOCKE's communications with his counsel in his pending matter. To be clear, neither these messages nor any others reviewed by law enforcement are subject to any attorney-client privilege; indeed, the messages that prompted this pause could not be subject to such a privilege, insofar as they are believed to be between Inmate LOCKE and a non-lawyer. Nevertheless, law enforcement, working with the United States Attorney's Office, has implemented a "filter team" and related protocol to inoculate against the risk that members of the prosecution team here would encounter privileged material.

Reason to Believe Multiple Devices Associated with 414-388-9559 and 414-242-1974 will Contain Evidence of the Subject Offenses

33. Further, there is probable cause to believe that records of HAMDHA's commission of the SUBJECT OFFENSES will be found on electronics associated with 414-388-9559 and 414-242-1974, described in Attachment B.

34. As previously indicated in this Affidavit, there is probable cause to believe DEBERRY used 414-982-9371 to communicate with Inmate LOCKE's associates, to include HAMDHA on 414-388-9559 and 414-242-1974, on days relevant to the SUBJECT OFFENSES. Indeed, on March 22, 2023, the same day the phone located in Inmate LOCKE's cell was activated, DEBERRY was observed interacting with the operator of Target Vehicle-1, believed to be HAMDHA, just 15 minutes after Target Vehicle-1 was observed parking in the Waukesha County Jail parking lot. I am also unaware of any evidence suggesting HAMDHA and DEBERRY communicated regarding the delivery using some other means not involving 414-982-9371, 414-388-9559 , and 414-242-1974. And based on my training and experience, people commonly use their cellular device to communicate when they have arrived at a location and to otherwise

coordinate their schedules. Further, and as indicated in footnote 1 above, DEBERRY used 414-982-9371 to communicate with HAMDHA on 414-388-9559 and 414-242-1974 on March 23, 2023 – the day after HAMDHA is believed to have provided DEBERRY with the cellphone that was found in Inmate LOCKE's cell.

35. Also, as previously indicated in this Affidavit, HAMDHA communicated with Inmate LOCKE using 414-388-9559 and 414-242-1974 hundreds of times between March 25, 2023 and April 13, 2023, while Inmate LOCKE was believed to be in possession of the cellular telephone HAMDHA provided to DEBERRY on March 22, 2023.

36. On June 16, 2023, SA Evertz served a subpoena upon Apple, Inc., requesting iCloud account information associated with the telephone numbers utilized by HAMDHA, 414-388-9559 and 414-242-1974. On June 30, 2023, Apple provided SA Evertz with electronic records in response to this subpoena. Within Apple's records, SA Evertz identified the following details linked to the iCloud account associated with 414-388-9559:

- DSID (unique Apple iCloud ID number): 10044014201
- Apple Logon ID: dynaabu18@gmail.com
- Account Creation Date: December 16, 2015
- Mailing Address: 5890 Tower Rd, Greendale, WI[2]
- Apple Devices Associated with DSID: Four (4) devices

37. With respect to 414-242-1974, SA Evertz identified the following iCloud account details:

[2] This address contains the identical street name and number with respect to the Target Residences, absent an apartment number.

- DSID: 20903152987
- Apple Logon ID: drtransportation@icloud.com
- Account Creation Date: January 16, 2023
- Mailing Address: 5890 Tower Road, #4, Greendale, WI (Target Residence-1)
- Apple Devices Associated with DSID: One (1) device

Physical Surveillance of the Target Residences and Target Vehicles

38. Beginning July 24, 2023, ATF SAs began surveilling the Target Residences as well as the Target Vehicles at 5890 Tower Road, Greendale, WI. On the following dates (July 24, 2023, July 25, 2023, July 26, 2023, and July 27, 2023), SAs observed a black 2023 Toyota Camry bearing WI tag "AFH5270" (Target Vehicle-1) and a white 2011 Dodge Caravan bearing WI tag "ASC6335" (Target Vehicle-2) parked directly in front of the apartment complex wherein the Target Residences are located. At approximately 10:20 AM, SA Erlien observed HAMDHA walk out of the 5890 Tower Rd apartment complex and get into Target Vehicle-2. HAMDHA was observed utilizing keys to enter the driver's seat of Target Vehicle-2before she moved the vehicle closer to the apartment complex. After this repositioning, HAMDHA exited Target Vehicle-2 and then entered the driver's seat of Target Vehicle-1 before departing the residence in Target Vehicle-1.

39. SAs referenced WI Department of Transportation (DOT) records and identified Target Vehicle-1 was most recently registered to HAMDHA on December 6, 2022. At the time of this registration, HAMDHA listed 5890 Tower Road, Apartment 4, Greendale, WI (Target Residence-1) as her residential address with WI DOT. With respect to Target Vehicle-2, WI DOT records identified the vehicle was registered to D&R Transportation LLC. Through information

gleaned over the course of the preceding and current investigations, SA Evertz believes "D&R" to stand for "Dyna and Ramone [LOCKE Sr.]." Target Vehicle-2's registration was renewed on December 6, 2022. WI DOT records identified D&R Transportation LLC's mailing address as 5890 Tower Road, Greendale, WI.[3]

40. SAs referenced WI Department of Financial Institutions (DFI) records, identifying D&R Transportation LLC was registered with WI DFI on October 30, 2022. WI DFI records also provided HAMDHA was the Registered Agent for D&R Transportation LLC, and HAMDHA had provided 5890 Tower Rd, Greendale, WI, as the Registered Agent Office address. WI DFI records also provided that HAMDHA was the Registration Agent for two (2) additional LLCs in WI:

- DTRANSPORTATION LLC
    - Date Organized (registered): March 18, 2023
    - Registered Agent Office Address: 5890 Tower Road, Apartment 4, Greendale, WI, 53129 (Target Residence-1)
- DYNA'S HOME IN CARE LLC
    - Date Organized: June 7, 2021
    - Registered Agent Office Address: 5890 Tower Road, Greendale, WI 53219

41. It is important to note that during the preceding ATF investigation, Investigators identified LOCKE Sr. was the Registered Agent for two LLCs, Amil promotions LLC and Amir Properties LLC. SA Everts knows through knowledge, training, and experience that narcotics

[3] This address contains the identical street name and number with respect to the Target Residences, absent an apartment number.

traffickers as well as individuals engaged in fraudulent criminal activities often utilize corporate structures (i.e., an LLC), to launder ("clean") their ill-gotten proceeds ("dirty money") or otherwise evade detection by law enforcement.

Undercover Interaction with HAMDHA on July 27, 2023

42. On July 27, 2023, ATF SAs, acting in an undercover capacity, conducted surveillance at 5890 Tower Rd, Greendale, WI. The undercover SAs contacted one of the lower-level unit tenants at 5890 Tower Road, asking if the tenant or someone in their building owned the white Dodge Caravan (Target Vehicle-2) parked on the street in front of the apartment complex. It is important to again note that Target Residence-1 and Target Residence-2 are two units on the second floor of the encompassing apartment complex at 5890 Tower Road. The undercover SAs explained to the lower-level tenant that the SAs needed the van moved off of the roadway (Tower Road), so the SAs could conduct geographic measurements on the roadway. The resident of the lower-level unit stated that they believed Target Vehicle-2 belonged to the resident of Unit No. 3 (Target Residence-2), which is located on the top floor (2nd story) of the apartment complex.

43. The undercover SAs then walked up the open stairway to make contact at Target Residence-2. Upon reaching the second floor, the undercover SAs observed that Target Residence-2 had a several pairs of tennis shoes near the door and had a doorbell security camera installed on the righthand side of the unit's door. The undercover SAs observed Target Residence-1 and Target Residence-2 were located directly across a small hallway from one another. In an effort to detect if anyone besides HAMDHA resided at Target Residence-1, the undercover SAs knocked on the door of Target Residence-1 numerous times but received no answer. The undercover SAs then knocked on the door of Target Residence-2 approximately two to three times before a voice (which

the SAs later confirmed to be that of HAMDHA's) answered through the doorbell camera voice system. HAMDHA greeted the undercover SAs and stated she was not home but was close by. The undercover SAs explained their ostensible purpose for being at the residence and explained they needed the owner of the white van (Target Vehicle-2) to move the vehicle for a brief period while the undercover SAs carried out their work on the roadway. It should be noted that the undercover SAs offered to come back at a later time if HAMDHA did not wish to immediately return to the apartment. HAMDHA confirmed she controlled Target Vehicle-2 and that she would return to the apartment complex within a few minutes. The undercover SAs then exited the apartment complex and awaited HAMDHA's arrival.

44. Approximately five minutes later, with the undercover SAs now outside, HAMDHA returned to apartment complex in Target Vehicle-1. Once HAMDHA parked Target Vehicle-1, she walked inside the apartment complex before she returned outside with a set of car keys approximately 1-2 minutes later. HAMDHA then temporarily moved Target Vehicle-2 and engaged in general conversation the undercover SA standing closest to her. After approximately two minutes, the undercover SAs thanked HAMDHA for her assistance and explained they had finished their work on the roadway. HAMDHA returned Target Vehicle-2 to its previous parking spot on the roadway before she reentered Target Vehicle-1 and departed the area.

Background Concerning Apple Devices[4]

45. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

46. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

- Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected

[4] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet- connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags,

which are tracking devices sold by Apple.

- Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

47. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple- provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

48. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

49. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

50. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial

number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

51. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

52. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. These stored communications and files connected to an Apple ID may be found on multiple Apple devices (iPhones, iPads, iPods, Laptop Computers, etc.).

53. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

54. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

TECHNICAL TERMS

55. Based on my training and experience, I use the following technical terms to convey the following meanings:

- Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and

moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users

can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

56. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I believe that HAMDHA's devices associated with telephone numbers 414-388-9559 and 414-242-1974 have capabilities that allow each to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

57. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

58. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how those devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on HAMDHA's devices associated with telephone numbers 414-388-9559 and 414-242-1974 because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

59. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of HAMDHA's devices associated with telephone numbers 414-388-9559 and 414-242-1974 consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether that part constitutes evidence described by the warrant.

60. *Manner of execution.* Because this warrant seeks permission to forensically examine devices that will, after their seizure, be in law enforcement's possession, I submit there is reasonable cause for the Court to authorize that the forensic examination portion of the warrant at any time in the day or night.

61. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

62. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a

combination of these biometric features, and the user of such devices can select which features they would like to utilize. Therefore, I request that this warrant permit law enforcement agents to obtain from HAMDHA the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that HAMDHA's physical biometric characteristics will unlock.

63. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

64. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

65. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

66. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

67. As discussed in this Affidavit, your Affiant has reason to believe that HAMDHA's devices associated with telephone numbers 414-388-9559 and 414-242-1974 are subject to search and seizure pursuant to the applied-for warrant. The passcode or password that would unlock the devices associated with 414-388-9559 and 414-242-1974 are currently not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within devices associated with 414-388-9559 and 414-242-1974, making the use of biometric features necessary to the execution of the search authorized by this warrant.

68. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to obtain from HAMDHA the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

CONCLUSION

69. Based upon the foregoing, I believe there is probable cause to believe that HAMDHA and other individuals have committed violations of federal law, including Title 18, United States Code, Sections 371, 1512, and 1791 (the "Subject Offenses"). I further submit that there is probable cause to believe that located at the Target Residences, Target Vehicles, and HAMDHA's person, described in Attachment A, there is evidence of the Subject Offenses, as detailed more specifically in Attachment B, such that a warrant should issue authorizing the search of the same.

ATTACHMENT A

Matter No. 2023R00184

The person to be searched pursuant to this warrant is Dyna Abu HAMDHA (F/W; DOB: 05/18/1991).

The places to be searched pursuant to this warrant are residences and conveyances utilized by HAMDHA; specifically:

a) 5890 Tower Road, Apartment 4, Greendale, WI (Target Residence-1);
   - Target Residence-1 is an apartment unit (No. 4) located on second floor within the southwest quadrant of the apartment complex located at 5890 North Tower Road. The main entrance to the encompassing building is located on the west side of the apartment complex, facing Tower Road. The entry door of Target Residence-1 is located directly across a small hallway from Target Residence-2.

b) 5890 Tower Road, Apartment 3, Greendale, WI (Target Residence-2);
   - Target Residence-2 is an apartment unit (No. 3) located on second floor within the northwest quadrant of the apartment complex located at 5890 North Tower Road. The main entrance to the encompassing building is located on the west side of the apartment complex, facing Tower Road. The entry door of Target Residence-2 is located directly across a small hallway from Target Residence-1.

c) 2023 Toyota Camry WI license plate "AFH5270" (Target Vehicle-1)
   - The Toyota Camry is dark black in color and possesses darkened windows. The vehicle also possesses dark gray/black rims. The vehicle's license plate bears WI tag "AFH5270."

d) 2011 Dodge Grand Caravan WI license plate "ACS6335" (Target Vehicle-2)
   - The Dodge Caravan is white in color, possessing a small amount of rust along the wheel wells and fuel tank inlet. The vehicle's license plate bears WI tag "ASC6335."

Collectively, Target Vehicle-1 and Target Vehicle-2 are the Target Vehicles.

Collectively, Target Residence-1 and Target Residence-2 are the Target Residences.

ATTACHMENT B

Matter No. 2023R00184

Evidence to be seized

All records, information and items, from HAMDHA, the Target Vehicles, or the Target Residences, that relate to violations of 18 U.S.C. §§ 371, 1512, and 1791 and involve Dyna Abu HAMDHA since January 1, 2023, including:

a. Records and information relating to contraband being provided to federal inmates;

b. Records and information relating to controlled substances;

c. Records and information relating to communications between Michael Wright, Ramone Locke, Amanda Deberry, and Dyna Abu Hamdha;

d. Records and information relating to communications with Michael Wright and/or Ramone Locke regarding their pending investigations;

e. Records and information relating to Michael Wright's pending case, Ramone Locke's pending case, or the obstruction of justice;

f. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Amanda Deberry, Michael Wright, Ramone Locke, and Dyna Abu Hamdha;

g. Records and information relating to the identity or location of the suspects, associates, and co-conspirators.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

For any computer or storage medium (including cellular phones) whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

During the execution of the searches described in Attachment A, law enforcement personnel are authorized to obtain from Dyna Abu HAMDHA the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock devices associated with 414-388-9559 and 414-242-1974, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, for the purpose of attempting to unlock 414-388-9559 and 414-242-1974's security features in order to search the contents as authorized by this warrant.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by

any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF or FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Dyna Abu Hamdha's person (DOB: 05/1991), residences and vehicles; See Attachments

Case No. 23 MJ 130
Matter No.: 2023R00184

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A; over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 8/14/2023 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. William E. Duffin.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/1/2023 at 11:31 AM

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Matter No. 2023R00184

The person to be searched pursuant to this warrant is Dyna Abu HAMDHA (F/W; DOB: 05/18/1991).

The places to be searched pursuant to this warrant are residences and conveyances utilized by HAMDHA; specifically:

a) 5890 Tower Road, Apartment 4, Greendale, WI (Target Residence-1);
   - Target Residence-1 is an apartment unit (No. 4) located on second floor within the southwest quadrant of the apartment complex located at 5890 North Tower Road. The main entrance to the encompassing building is located on the west side of the apartment complex, facing Tower Road. The entry door of Target Residence-1 is located directly across a small hallway from Target Residence-2.

b) 5890 Tower Road, Apartment 3, Greendale, WI (Target Residence-2);
   - Target Residence-2 is an apartment unit (No. 3) located on second floor within the northwest quadrant of the apartment complex located at 5890 North Tower Road. The main entrance to the encompassing building is located on the west side of the apartment complex, facing Tower Road. The entry door of Target Residence-2 is located directly across a small hallway from Target Residence-1.

c) 2023 Toyota Camry WI license plate "AFH5270" (Target Vehicle-1)
   - The Toyota Camry is dark black in color and possesses darkened windows. The vehicle also possesses dark gray/black rims. The vehicle's license plate bears WI tag "AFH5270."

d) 2011 Dodge Grand Caravan WI license plate "ACS6335" (Target Vehicle-2)
   - The Dodge Caravan is white in color, possessing a small amount of rust along the wheel wells and fuel tank inlet. The vehicle's license plate bears WI tag "ASC6335."

Collectively, Target Vehicle-1 and Target Vehicle-2 are the Target Vehicles.

Collectively, Target Residence-1 and Target Residence-2 are the Target Residences.

ATTACHMENT B

Matter No. 2023R00184

Evidence to be seized

All records, information and items, from HAMDHA, the Target Vehicles, or the Target Residences, that relate to violations of 18 U.S.C. §§ 371, 1512, and 1791 and involve Dyna Abu HAMDHA since January 1, 2023, including:

a. Records and information relating to contraband being provided to federal inmates;

b. Records and information relating to controlled substances;

c. Records and information relating to communications between Michael Wright, Ramone Locke, Amanda Deberry, and Dyna Abu Hamdha;

d. Records and information relating to communications with Michael Wright and/or Ramone Locke regarding their pending investigations;

e. Records and information relating to Michael Wright's pending case, Ramone Locke's pending case, or the obstruction of justice;

f. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Amanda Deberry, Michael Wright, Ramone Locke, and Dyna Abu Hamdha;

g. Records and information relating to the identity or location of the suspects, associates, and co-conspirators.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

For any computer or storage medium (including cellular phones) whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

During the execution of the searches described in Attachment A, law enforcement personnel are authorized to obtain from Dyna Abu HAMDHA the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock devices associated with 414-388-9559 and 414-242-1974, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, for the purpose of attempting to unlock 414-388-9559 and 414-242-1974's security features in order to search the contents as authorized by this warrant.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by

any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF or FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.